Attachment 1 to
IHC-MM-296
17 February 1972

IBSEC-CSS-R-9
11 FEB 1972

UNITED STATES INTELLIGENCE BOARD

SECURITY COMMITTEE

MEMORANDUM FOR: Chairman, Intelligence Information Handling Committee, United States Intelligence Board

SUBJECT : Guidelines for ADP Disaster Prevention and Contingency Back-up Planning

1. The attached "Guidelines for ADP Disaster Prevention and Contingency Back-up Planning" were developed by the Computer Security Subcommittee in coordination with the Support Staff of the Intelligence Information Handling Committee. The Security Committee approved these Guidelines at its 25 January 1972 meeting.

2. The Guidelines are intended for the use of USIB member agencies in ensuring against disruption of the computer processing and exchange of vital information. Throughout their development no consideration has been given to making them directive in nature.

3. Subsequent to IHC review and approval, I would propose their issuance and dissemination as a joint product of the SECOM and IHC.

[redacted]

25X1

Howard J. Osborn
Chairman, Security Committee
USIB

Att

GUIDELINES FOR ADP DISASTER PREVENTION

AND CONTINGENCY BACK-UP PLANNING IBSEC-CSS-R-9

25 Jan 72

I. PURPOSE

To provide basic guidance for the development of a disaster prevention and contingency back-up program for insuring the continuous computer processing and exchange of vital information. To outline the major areas of concern and list conditions and procedures necessary to insure the protection of ADP assets. To list actions and procedures for consideration in the formulation of a contingency plan.

II. APPROACH

Guidance set forth herein is based on the premise that organizations relying heavily on computer system operations should develop an integrated ADP Disaster Prevention and Contingency Back-Up Program to minimize the severity and effects of unforeseen computer system disasters. Such planning should be a specific design factor integrated into total system planning for each individual system and its unique environment.

III. GENERAL CONSIDERATIONS

Potential causes of disaster vary considerably in their

probability of occurrence, degree of criticality and feasibility of preventive and/or back-up measures. Fires, explosions, toxic fumes, nuclear weapon detonation and the effects of natural disasters such as earthquakes, hurricanes and floods can be immediately disastrous resulting in the death or serious injury to personnel. The damage caused by such events to computer equipment, the physical structure housing the system, and the storage media may be disastrous for an extended period of time depending upon resource recovery capabilities. Other disruptive events such as outages of electric power or air conditioning, the loss of telecommunications facilities or the erasure of vital information from magnetic storage media are not likely to be as serious because back-up measures can be provided. Although positive security actions and procedures can reduce the effects of riots, theft, sabotage and vandalism, these events can occur and result in disastrous operating consequences.

IV. DISASTER ANALYSIS

A disaster includes any incident or event which results in a critical disruption of the computer operations. Rescheduling of work loads according to user priority may be required depending upon the allowable delay of the most critical user processing requirements. Processing priorities may also be required if the disruption results in partial

operability of the system. The disruption can reach major proportions rendering the system inoperable for a prolonged period of time and requiring movement of highest priority processing to an alternate computer site.

The emergency or back-up actions needed to restore the capabilities of a computer system after a disaster has occurred should be proportionate to the critical effects of that disaster. These actions may be identified through consideration of at least the following:

1. The event, cause or condition creating the disruption;

2. The capability to restore the system;

3. The total period of time the system is expected to be nonoperational;

4. The tolerable time-limits of system inactivity based on user requirements;

5. The feasibility of a degraded mode of system operation whereby critical processing could continue; and

6. The availability of an alternate system capable of assuming the critical processing requirements for a specified period of time.

V. MAJOR AREAS OF CONCERN AND PREVENTIVE MEASURES

The major areas of concern involve the protection of assets required for computer operation. The protection of ADP assets requires the implementation of various measures as part of a disaster prevention program. Security and

computer personnel should be alert to the possibility that a disruption in computer activity may be deliberate rather than accidental and should investigate any situation where such evidence exists. Although the configuration of computer systems and the physical environment of computer centers vary, the following areas are applicable to all systems:

1. System Hardware: The mechanical, electromechanical, electronic, magnetic and electrical components of a computer system.

a. Maintenance: Effective maintenance planning represents the initial preventive measure against a potentially serious disruption of operations.

b. Engineering Support: Technical support should be available on a 24 hour on-site basis if the computer center requires such support. Back-up of critical hardware parts should be maintained on-site or in a readily accessible location.

c. Hardware Security: The implementation of measures such as memory protection and user/executive modes of operation is recommended to insure protection of user data sets.

2. System Software: Computer programs and procedures including system and user programs.

a. Testing a New Installation: Duplicate programs should be run on both the current and proposed system so

that the data can be compared. If duplicate testing is not feasible, a test deck should be used to check the system's logic.

b. Program Changes and Testing: Extensive program debugging is recommended to reduce the number of disruptions caused by software errors. Any request for a program change should be submitted in writing and the action authorized only by a responsible manager. The number of persons authorized to make changes in operating programs should be limited. Program testing should be subject to review by authorized personnel and not conducted solely by the person who wrote the program.

c. Software Security: Software security measures such as user identification and authorization should be used to reduce the possibility of unauthorized personnel accessing the system.

3. System Operational Personnel: The individuals whose primary duties are concerned with the operation of the computer system.

a. Selection of Key Personnel: Key personnel designated to continue the operation of a computer system should be briefed and provided written guidance as to their responsibilities and duties in the event of a disaster.

b. Training of Key Personnel: Training programs should be developed which stress the proper handling and maintenance of computer system components. Key personnel

should be broadly cross-trained in the event that certain key personnel should be unable to respond to an emergency situation.

c. Personnel Security: Computer personnel, visitors and users constitute a theft and/or sabotage threat to the computer center. Restrictions on the number of people allowed unescorted access and on the areas to which they have access are recommended.

4. System Environment: The computer facility, supporting utilities and operational posture.

a. Facility (General): The facility housing a computer system should be constructed of fire resistant building materials and equipped with appropriate smoke detection, heat sensing and fire fighting devices. Periodic safety checks of such devices for their operational capability is encouraged. The use of the FPMR and the National Fire Code volume 5, section 75 is recommended in the construction of computer facilities. Consideration should be given to maximum physical protection against the potentially catastrophic effects of natural disasters (hurricanes, earthquakes and floods) as well as civil disorder and conventional and nuclear warfare.

b. Auxiliary Power and Air Conditioning: Malfunctions and failures of electric power and/or air conditioning are two of the major causes of disaster affecting a computer system. Provisions should be made for

the use of an independent back-up power source as well as providing for immediate repair or replacement of air conditioning equipment. Consideration of line monitors and/or overvoltage protectors to prevent damage from power failure and power surges is recommended. Security controls should be applied to reduce the possibility of willful or inadvertent damage to the electrical and air conditioning equipments.

c. Physical Security and Control: Access to the facility housing the system by other than authorized personnel should be prohibited. The mechanisms installed to enhance the security of the computer system area should be controlled by personnel designated as responsible for their maintenance and integrity. All procedures relating to facility control should be in writing and made available to assigned personnel.

5. Data Files: Storage areas for magnetic storage media should be located outside the main computer area, preferably in a vault or secure area depending upon security considerations. Proper temperature and humidity should be maintained and cleanliness restrictions should be observed. All appropriate executive programs, system documentation, operation manuals, etc., required for the computerized processing of information should be identified, duplicated, and safely stored. Security procedures should be installed to prevent unauthorized personnel from removing files such

as magnetic tapes from the computer center.

6. Communication Lines: Requirements for protecting communication lines will vary depending upon the existence and location of remote terminals. The communication links from the central processor to the remote consoles are vulnerable to crosstalk, electromagnetic radiation and wiretaps. Unprotected data transmission should be eliminated by use of cryptographic techniques or by physical security measures. Back-up communication facilities should be available to reduce the effect of failures in the communication area.

7. Supplies: Supplies that are essential to computer operations should be identified and accessibility to back-up supplies should be provided.

VI. CONTINGENCY PLANNING

A manual or handbook detailing the computer center methods of operation in the event of a disaster should be prepared. It should specify the contingency or back-up actions to be taken, individual responsibilities for these actions and the follow-on investigative and reporting requirements. The degree of implementation of the contingency plan will depend upon the criticality of the disaster.

Planning for possible emergencies should consider the recommendations listed below for disaster prevention and/or coping with disasters which have occurred.

A. Prior Planning

1. Duplication and storage of vital programs, documentation and data files in a readily accessible location, preferably off-site.

2. A determination that the fire safety equipment and emergency plans are adequate to minimize damage from smoke, chemicals, water or fire.

3. A determination that adequate electrical power, air conditioning equipment, and heating systems are available for back-up use.

4. Training of computer personnel to insure that they are aware of proper procedures for operating and protecting equipment and are aware of their responsibilities in the event of a disaster.

5. Up-to-date lists of emergency and support organizations and personnel with whom contact may be required. This may include medical centers, fire stations, security services and equipment maintenance services.

6. All data being processed should bear a priority of processing order. Users should be alert to the need for manual information processing in the event computer processing is not available for low priority processing.

7. Copies of all disaster planning documentation should be provided to each major functional area supporting the organization. Specific roles and responsibilities of each supporting function should be closely coordinated.

8. The contingency plan should be updated periodically to reflect changes in equipment, user requirements, personnel, and back-up computer compatibility and availability.

B. Major Disaster Planning- Contingency planning for a major disaster which requires movement of computer processing activities to an alternate site should also consider the following recommendations:

1. Prior identification of an alternate computer system compatible with in-house systems that can be available if needed. Physical surrondings of the alternate system should conform to required security and safety standards.

2. Identification and designation of personnel to manage and operate the alternate system should be documented and updated as the need arises.

3. The computer operations at the alternate site should be carefully documented. Among other issues, this document should address such items as the transportation of alternate site computer personnel, their responsibilities during alternate site operations, the necessary security considerations for the computer environment and the transfer of classified data to the alternate site, and the priority processing order of data.

4. Periodic operation of the alternate computer system using the duplicate documentation, software and data files by the designated alternate system personnel should be made. Results should be compared with normal operations in order for changes to be effected if required.

5. Instructions for the destruction of classified data and/or equipment under combat-emergency conditions where such classified materials may be reasonably expected to fall into the possession of unauthorized persons.

C. Post Disaster Planning

1. A determination of the criticality of the disaster considering anticipated time of system inoperability and user processing requirements.

2. Immediate notification to management and system users of the estimated length of delay in operations to allow the users to consider alternate operational methods.

3. Notification of the appropriate higher levels of management if the time delay exceeds initial estimates.

4. Contact with the appropriate emergency and support organizations depending upon the cause and extent of the disaster.

5. A determination of the feasibility of continued computer operation in a degraded mode.

6. Initiation of actions to move computer operations to an alternate site if conditions warrant the move.

7. A determination that the disaster has not degraded the essential system hardware, software or physical security features and that procedural security controls remain in effect.